Robust quantum cryptography with a heralded single-photon source based on the decoy-state method

Qin Wang[1,2],* Wei Chen[1], Guilherme Xavier[2], Marcin Swillo[2], Tao Zhang[1], Sebastien Sauge[2], Maria Tengner[2], Zheng-Fu Han[1], Guang-Can Guo[1], and Anders Karlsson[2]

[1]*Department of Physics, Key Laboratory of Quantum Information, CAS, USTC, 230026, Hefei, China and*

[2]*Department of Microelectronics and Applied Physics, Royal Institute of Technology (KTH), Electrum 229, SE-164 40 Kista, Sweden*

Abstract

In this paper, we describe a robust quantum cryptography scheme with a heralded single photon source based on the decoy-state method, which has been shown by numerical simulations to be advantageous compared with many other practical schemes not only with respect to the secure key generation rate but also to secure transmission distance. We have experimentally tested this scheme, and the results support the conclusions from numerical simulations well. Although there still exist many deficiencies in our present systems, it's still sufficient to demonstrate the advantages of the scheme. Besides, even when cost and technological feasibility are taken into account, our scheme is still quite promising in the implementation of tomorrow's quantum cryptography.

PACS number(s): 03.67.Dd, 42.65.Yj, 03.67.Hk

*Electronic address: qinw@kth.se

I. INTRODUCTION

Cryptography plays an important role in the field of communication, the goal of it is to render messages between legitimate users (usually called Alice and Bob) but incomprehensible to Eve (a malicious eavesdropper). However, classical cryptography is based on conjectured computational complexity, and its security is thus threatened by the advancement in mathematical algorithms and computational power. Compared with the classical method, quantum cryptography has unprecedented advantages because it does not based on computational complexity, and its unconditional security is ensured by the "battle tested" theory of quantum mechanics [1–5].

Since the first protocol of quantum cryptography was put forward by Bennett and Brassard in 1984 [1], (hereafter called BB84 protocol,) quantum cryptography has been widely investigated and developed by large numbers of researchers and scientists, not only in theory, but also by experimental implementations. Unfortunately, there always exists some discrepancies between the "in principle" unconditional security and realistic systems. Therefore, people have to take practical usability into account when estimating a quantum cryptosystem, just as summarized in Ref. [6]:

$$\begin{aligned} \text{Infinite security} &\Rightarrow \text{Infinite cost} \\ &\Rightarrow \text{Zero practical interest.} \end{aligned} \tag{1}$$

In current practice, an attenuated laser (*i.e.,* emitting a weak coherent state WCS) or a parametric down-conversion source (PDCS) are employed in most quantum cryptosystems. A WCS is quite easy to implement. However, it contains a large vacuum state probability amplitude and unneglectable multiphoton probability amplitude when attenuated to a single photon level, which is fatal to photon-number-splitting (PNS) attack [7–10] and some other attacks. To compensate the security, one has to attenuate a laser into a quite low intensity (*e.g.* 0.1 photon/ pulse), resulting in a low secure key generation rate and a limited transmission distance.

Fortunately, the so-called decoy-state method was given out [11–13]. The main idea of the decoy-state method is to randomly mix extra decoy transmission events with the true signal transmission events. The decoy transmission events and the signal transmission events

have the same characteristics (such as wavelength, bandwidth and timing information, etc.) except for different intensities. Therefore, for a given random photon state, Eve is unable to judge whether it comes from a decoy transmission event or from a signal transmission event. Hence she has to perform the same operations on them. On the other hand, the legitimate users, Alice and Bob, could estimate the behavior of vacuum, single-photon and multi-photon states individually just by doing some counting measurements and classical communications. As a result, Eve's eavesdropping with be detected. It has been shown that the decoy-state method has significantly improved the performance of a quantum cryptography with practical systems.

The heralded single-photon source (HSPS) from parametric down-converted (PDC) processes has also been widely investigated in recent years [14–18]. Its sub-Poissonian photon number distribution makes it suitable for the implementation of quantum cryptography. (It has already been proven that a sub-Poissonian distributed source is superior to a Poissonian one in the quantum cryptography [19].)

Combining the advantages of the decoy state method and the HSPS, we have proposed some schemes that applies both of them in a quantum cryptography setup [20–23]. In Ref. [20–22], only theoretical aspects are discussed (for simplicity, those models in them all assumed some ideal conditions, *i.e.* the idler and the signal photons in different paths have the same photon distributions before being detected. However, they can be quite different in practice because of existing coupling loss and some other factors.). In Ref. [23], some preliminary experimental results are presented. Here in this paper, we will describe our theory and experiment in detail and include some experimental improvements as well.

This paper is organized as follows: At first, in section II, we will introduce some basic theory on HSPS and report some experimental results from our group; In section III, we will introduce our scheme in detail, and also do some numerical simulations to show the advantages of our scheme compared with other practical schemes; In section IV, we will describe our experimental setup and experimental processes, and compare our experimental results with theoretical predictions; Subsequently, we will discuss some deficiencies existing in our present systems, and then make suggestions on how to improve them in section V; Finally, the conclusions are drawn and the future prospects are spelled out.

II. THEORY AND EXPERIMENT IN HSPS

In recent years, a HSPS based on a PDC process has been investigated by many groups. With improvements of down conversion in waveguides and four-wave mixing, a lot of encouraging results have been reported [14–18].

The main idea of the HSPS is to use one photon (heralding) of a photon pair to announce the arrival of the other one (heralded). The temporal statistics of a HSPS can be controlled by utilizing a *prior information* (*i.e.,* original distribution) extracted from the photon pairs. As said in Ref. [14], during the nondegenarate spontaneous parametric down conversion (SPDC) process, if a pulsed pump laser is used, as long as the coherence time of the emission, Δt_c, is much longer than the duration of the pump pulse, Δt, *i.e.,* $\Delta t_c \gg \Delta t$, (in practice easily obtained by using ultrafast (fs) pulse pump lasers), a single emission process will take place, giving an thermal photon number distribution. In contrast, when a continuous wave (CW) laser is used, as long as Δt_c is much shorter than the gating period of the detector, a large number of independent SPDC processes will be present, each thermally distributed, but collectively resulting in a Poisson distribution. However, the "original" distribution can be altered by conditional gating. By choosing proper gating time and using an appropriate correlation rate, a sub-Poissonian distributed HSPS can be obtained as the result of postselections.

To quantify our source, let us introduce the second-order auto-correlation function at zero-time delay:

$$g^{(2)}(0) = \frac{2P_{m\geq 2}}{P^2_{m\geq 1}}. \tag{2}$$

(It is known that, the value of $g^{(2)}(0)$ could be used to classify a source between a Poisson ($g^{(2)}(0) = 1$), a sub-Poisson ($g^{(2)}(0) < 1$) and a super-Poisson ($g^{(2)}(0) > 1$) distribution.) $P_{m\geq k}$ is the probability to find at least k photons within a gating period, which can be expressed as:

$$P_{m\geq k} = P^{cor} P^{acc}_{m\geq k-1} + (1 - P^{cor}) P^{acc}_{m\geq k}, \tag{3}$$

where P^{cor} is the correlation rate of photon pairs, *i.e.* the probability that we can predict the existence of a heralded photon when a heralding one was detected. (Its value equals unity under perfect experimental conditions, *i.e.,* when there is no coupling loss, no transmission loss, and no detection loss etc.) $P^{acc}_{m\geq k}$ is the probability that at least k accidental photons are present within a gating period, which comes from the "original" statistical distribution

of the down-converted light (the coherence time of the single photons ($\Delta t_c \sim 10$ ps) is much less than the integration time (2.5 ns), as a result, those signal photons which are not coming from the same SPDC process as the heralding one (it means they are not truly correlated photon pairs) may also contribute to the final coincidence counts.). It is given by:

$$P_{m\geq k}^{acc} = 1 - \sum_{i=0}^{k-1} \frac{\mu^i}{i!} e^{-\mu}, \quad (k \geq 2) \tag{4}$$

where μ is the average photon number per gating time (before detection), $\mu = R_s \cdot \Delta t_{gate}$, R_s is the mean photon number per second (before detection), and Δt_{gate} is the gating time of the detector.

Moreover, the probability of getting exactly n photons within the gating time is:

$$P(n) = P_{m\geq n} - P_{m\geq n+1}, \quad (n \geq 2). \tag{5}$$

To be noted, the vacuum state probability should be treated independently, which can be stated as:

$$P(0) = P^{cor} \cdot d_i + (1 - P^{cor}) \cdot e^{-\mu}, \tag{6}$$

where d_i is the dark count probability of the detector for heralding photons.

Consequently, the single-photon probability is:

$$P(1) = 1 - P(0) - P_{m\geq 2}. \tag{7}$$

Considering Eqs. (2)-(7), in order to analyze a HSPS, we should at first get to know the values of P^{cor} and μ. In the following, we will explain how their values can be determined in an experiment.

Our experimental setup for the HSPS is shown in Fig. 1. We use a CW laser at the wavelength of 532 nm to pump a periodically-poled $LiNbO_3$ (PPLN) crystal of 50 mm length to generate non-degenerate correlated photon pairs. The photon at the wavelength of 809 nm is called idler, and the one at the wavelength of 1555 nm is called signal. After separation by a dichroic mirror (DM), they are coupled into different detectors. For the idler photons, we used a Si-based APD (PerkinElmer SPCM-AQR-14) with a detection efficiency of about 50%; for the signal photons, a InGaAs-APD (id200-SMF) operating in gated Geiger mode is used. Whenever there is an idler photon being detected, an electronical pulse is sent out. After the time chopper (TC, the details about it will be described in section IV), each

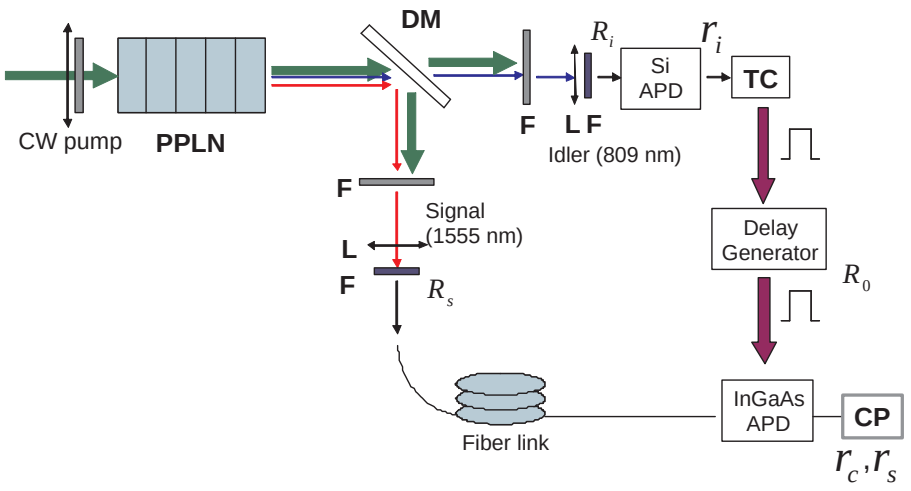

Fig. 1: (Color online) Schematics of the experimental setup to produce a HSPS. PPLN: periodically-poled $LiNbO_3$ crystal; DM: dichroic mirror; F: filter; L: lens; TC: time chopper; CP: counter processing; R_i and R_s are the photon rates inside the fibers for idler and signal respectively; r_i is the single photon counting rate at the Si-detector; R_0 is the triggering rate; r_c and r_s are the counting rates at the InGaAs detector triggered by idler photons and triggered by random pulses individually.

electronical pulse is used to trigger the InGaAs detector (with a gating time of 2.5 ns), then the coincidence count, r_c, will be obtained; r_i is the Si-detector single counting rate; r_s is the InGaAs detector single counting rate with random gating (the gating frequency is R_0), to provide the mean accidental photon number; R_0 is the heralding rate, whose value can be different from r_i, because of the dead/delay time of the pulse generator used; Besides, η_i (η_s) and d_i (d_s) are the detection efficiency and dark count probability of idler (signal) photons respectively; R_i (R_s) is the corresponding photon number for idler (signal) before detection.

When the InGaAs detector is randomly gated, the detection probability can be written as:

$$P_{\rm det}^{Ran} \equiv \frac{r_s}{R_0} = 1 - (1 - P^{acc})(1 - P_{dark}), \tag{8}$$

where P^{acc} ($= 1 - e^{-\eta_s R_s \Delta t_{gate}}$) and P_{dark} ($= \frac{d_s}{R_0}$) are the corresponding probabilities caused by accidental photons and dark counts.

Table I. The measured photon-number distributions of our HSPS under different triggering frequencies.

Trigger frequency (after time chopper, kHz)	Mean photon number (per gate, 2.5ns)	p_0	p_1	p_2	$g^2(0)$	P^{cor}
200	0.577×10^{-3}	0.566884	0.432830	2.85710×10^{-4}	3.046×10^{-3}	0.432837
650	5.325×10^{-3}	0.591017	0.406811	2.17189×10^{-3}	2.597×10^{-2}	0.405844

From these relations, it can be deduced that:

$$R_s = \frac{1}{\eta_s \Delta t_{gate}} \ln \frac{R_0 - d_s}{R_0 - r_s}. \tag{9}$$

When the InGaAs detector is gated by idler photons, the detection probability is:

$$P_{\rm det} \equiv \frac{r_c}{R_0} = 1 - (1 - P^{cor})(1 - P^{acc})(1 - P_{dark}), \tag{10}$$

because the detection events can be caused by correlated photons, accidental photons or dark counts. The equations above lead to:

$$P^{cor} = 1 - \frac{R_0 - r_c}{R_0 - d_s} e^{\eta_s R_s \Delta t_{gate}}. \tag{11}$$

Obviously, all the parameters in Eqs. (9) and (11) can be experimentally measured, giving the values of R_s and P^{cor}. By substituting them into Eqs. (2)-(7), we can finally calculate the photon number distribution of our source shown in Table I.

It can be seen from Table I that, because of a CW laser being used, the multi-photon probability of our source has substantially been depressed. By carefully optimizing the alignment of our optical systems, we can get a sub-Poissonain distributed HSPS with the single photon probability of about 40% (it's about 30% in [23]), which substantially improves the performance of a quantum cryptography as shown in Fig. 2.

III. QUANTUM CRYPTOGRAPHY WITH A HSPS BASED DECOY-STATE METHOD

Similarly to Ref. [20–22], we have used a three-intensity (μ', μ, μ_0) decoy-state method, where μ', μ and μ_0 are the mean photon number per gate for the signal light, the decoy light

and the "vacuum" light individually. The counting probabilities for μ' and μ can be written as:

$$Q_{\mu'} = \sum_{i=0}^{\infty} Y_n P_{\mu'}(n), \tag{12}$$

$$Q_{\mu} = \sum_{i=0}^{\infty} Y_n P_{\mu}(n), \tag{13}$$

Defining Y_n to be the yield of an n-photon state, *i.e.*, the conditional probability of a detection event at Bob's side given that Alice sends out an n-photon state, which is essentially a sum of two contributions, background and true signal, *i.e.,* $Y_n = Y_0 + 1 - (1-\eta)^n$. η is the combined detection efficiency and transmittance between Alice and Bob. Y_0 is Bob's background rate, which includes the detector dark count and other background contributions such as the stray light from timing pulses. The gain, G_n is the product of the probability of Alice sending out an n-photon state and the conditional probability of Alice's n-photon state, which is given by: $G_n = Y_n P(n)$. $P_{\mu'}(n)$ ($P_{\mu}(n)$) is the n-photon number probability in the source of μ' (μ).

Furthermore, the average quantum bit error ratios (QBER) for μ' and μ are given by:

$$E_{\mu'} = \frac{\sum_{i=0}^{\infty} Y_n P_{\mu'}(n) e_n}{Q_{\mu'}}, \tag{14}$$

$$E_{\mu} = \frac{\sum_{i=0}^{\infty} Y_n P_{\mu}(n) e_n}{Q_{\mu}}, \tag{15}$$

where e_n is the quantum bit error probability of an n-photon state.

Eq. (12) and (13) lead to:

$$\begin{aligned} & P_{\mu'}(2)Q_{\mu} - P_{\mu}(2)Q_{\mu'} \\ & = Y_0[P_{\mu'}(2)P_{\mu}(0) - P_{\mu}(2)P_{\mu'}(0)] + Y_1[P_{\mu'}(2)P_{\mu}(1) - P_{\mu}(2)P_{\mu'}(1)] \\ & + \sum_{i=2}^{\infty} Y_n[P_{\mu'}(2)P_{\mu}(n) - P_{\mu}(2)P_{\mu'}(n)]. \end{aligned} \tag{16}$$

Considering Eqs. (2)-(7) and the values of P^{cor} for μ and μ' in Table I, one can show that

for our setup $\sum_{i=2}^{\infty} Y_n(P_{\mu'}(2)P_\mu(n) - P_\mu(2)P_{\mu'}(n)) \leq 0$, which leads to:

$$Y_1 \geq \frac{P_{\mu'}(2)Q_\mu - P_\mu(2)Q_{\mu'} - Y_0(P_{\mu'}(2)P_\mu(0) - P_\mu(2)P_{\mu'}(0))}{(P_{\mu'}(2)P_\mu(1) - P_\mu(2)P_{\mu'}(1))},$$

$$e_1 \leq \frac{E_{\mu'}Q_{\mu'} - e_0 Y_0 P_{\mu'}(0)}{Y_1 p'_1(\mu')}.$$

When taking statistical fluctuations into account, we can get a lower bound for Y_1 and an upper bound for e_1:

$$Y_1^L = \frac{P_{\mu'}(2)Q_\mu^L - P_\mu(2)Q_{\mu'}^U - Y_0^U(P_{\mu'}(2)P_\mu(0) - P_\mu(2)P_{\mu'}(0))}{(P_{\mu'}(2)P_\mu(1) - P_\mu(2)P_{\mu'}(1))}, \tag{17}$$

$$e_1^U = \frac{E_{\mu'}Q_{\mu'}^U - e_0 Y_0^L P_{\mu'}(0)}{Y_1^L p'_1(\mu')}, \tag{18}$$

where $Q_\mu^L \equiv Q_\mu\left(1 - \frac{10}{\sqrt{N_\mu Q_\mu}}\right)$, $Q_{\mu'}^U \equiv Q_{\mu'}\left(1 + \frac{10}{\sqrt{N_{\mu'}Q_{\mu'}}}\right)$, $Q_{\mu'}E_{\mu'}^U \equiv Q_{\mu'}E_{\mu'}\left(1 + \frac{10}{\sqrt{N_{\mu'}Q_{\mu'}E_{\mu'}}}\right)$, $Y_0^L \equiv \left(1 - \frac{10}{\sqrt{N_0 Y_0}}\right)$, and $Y_0^U \equiv \left(1 + \frac{10}{\sqrt{N_0 Y_0}}\right)$ [24].

After error correction and privacy amplification, we can get the final key generation rate from the signal (μ') [25, 26]:

$$R \geq q\left\{-Q_{\mu'} f\left(E_{\mu'}\right) H_2\left(E_{\mu'}\right) + G_0 + G_1^L\left[1 - H_2\left(e_1^U\right)\right]\right\}, \tag{19}$$

where the factor q ($= \frac{1}{2}$) comes from the cost of basis mismatch in the Bennett-Brassard 1984 (BB84) protocol, (it's $\frac{1}{4}$ when a one-detector scheme is used), $f(E_{\mu'})$ is a factor represents the cost of error correction given existing error correction systems in practice. We use $f(E_{\mu'}) = 1.22$ here [8]; In addition, $G_0 \equiv Y_0 P_{\mu'}(0)$; $G_1^L \equiv Y_1^L P_{\mu'}(1)$; $H_2(x)$ is the binary Shannon information function, given by

$$H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x).$$

We have used decoy states in the above deduction processes for G_1^L and e_1^U. However, we will consider the case without decoy states in the following, in order to make a comparison. Without decoy state, we have to do a pessimistic assumption in the estimation of G_1^L and e_1^U, *i.e.,* we have to assume that the photons that fail to arrive at Bob's side all come from single photon states. As a result, we get the lower bound of G_1 as:

$$G_1^L = Q_{\mu'} - G_0 - \sum_{i=2}^{\infty} P_{\mu'}(n). \tag{20}$$

It's the same as Eq. (18), corresponding upper bound value of e_1 can also be obtained.

Using the formulas above and considering different distributions, we can give a comparison between our scheme using a HSPS based decoy-state method and other practical schemes, including using a HSPS but without decoy-state method, WCS with (or without) decoy-state method, and an ideal single photon source. For the sake of fairness, during the comparison in all the schemes, we use the BB84 protocol and assume the same experimental conditions, *i.e.,* the same dark count probability 0.8×10^{-5}/gate, the same detection efficiency 7.5%, and the same misalignment of the system $e_{\mathrm{det}\,ector} \sim 2.5\%$. Corresponding numerical simulation results are shown in Fig. 2. Clearly, compared with other practical schemes, our scheme can tolerate the highest total loss, that also means the highest key generation rate under fixed loss. Moreover, if a HSPS with 70 percent single photon probability (reported in [27]) is used, its performance can come close to the ideal single photon case.

IV. EXPERIMENTAL IMPLEMENTATION

Our experimental setup is shown in Fig. 3. Using the same structures as in Fig. 1, we can get a HSPS with narrow bandwidth (0.8 nm FWHM) and a single photon number probability of about 40% (see Table I). (The single photon probability is improved compared with before reported in [23]. Because here we use a new pump laser whose coherence length and spectrum has a little difference from the former one, which will inevitably influence the following focusing and collecting processes. On the other hand, the single photon probability obtained has close correlations with the final coincidence counting rate, and the final coincidence counting rate is so sensitive to the optical alignment and optical focusing settings. So we try to readjust the positions of focusing lenses and re-optimize the optical alignment, which result in an increased coincidence counting rate, and also an improved single photon probability.) Then the heralded single photons are transmitted from Alice to Bob through 25 km of spooled SMF-28 fiber (attenuation: 0.2 dB/km), incorporating a one-way Faraday-Michelson (F-M) cryptosystem [28]. We use a four-state [29] and one-detector phase-coding scheme, which is immune to time-shift attacks [30, 31], faked-state attacks [32], Trojan horse attacks [33], and can also been proven to be secure against any other standard individual or coherent attacks.

In order to generate down-converted light with three intensities (μ', μ, μ_0), on one hand

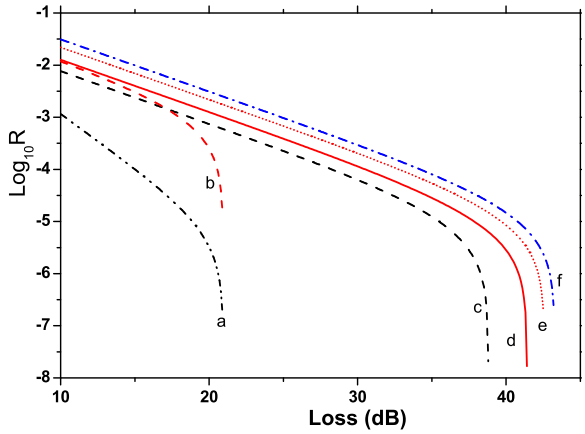

Fig. 2: (Color online) The key generation ratio vs. the total losses comparing several different schemes. The numerical simulations are done in the case of: a) With WCS and without decoy-state method. b) With HSPS and without decoy-state method; c). With WCS based decoy-state method (with optimal values of μ' at each point and an infinite number of decoy states). d) With HSPS based decoy-state method with P_{cor}=40% ($\mu' = 5.325 \times 10^{-3}$ and $\mu = 6.600 \times 10^{-4}$, these parameters come from our experiment. After numerical simulation, we also find the key ratio is stable with moderate variations of the value of μ' or μ). e) With HSPS based decoy-state method with P_{cor}=70% ($\mu' = 5.325 \times 10^{-3}$ and $\mu = 6.600 \times 10^{-4}$). f) With the ideal SPS. (Noted: For fair comparison, we consider using infinite number of signal pulses, so we don't take statistical fluctuation into account in all these lines above.)

we place an acousto-optic-modulator (AOM, 3.5 dB loss) in front of the PPLN crystal, on the other hand, we use a fiber pig-tailed optical switch (OS, 0.6 dB loss) at the arm of signal photons (1555 nm). By controlling both of them in our program (changing between μ' and μ with AOM, and changing between μ and μ_0 with OS), we can randomly generate signals with three different mean photon numbers: $[\mu', \mu, \mu_0] = [5.325 \times 10^{-3}, 0.660 \times 10^{-3}, 0.577 \times 10^{-5}]$. (Because of an imperfect isolation ratio of the optical switch ($\sim$ 20 dB), we don't produce a real vacuum state, but generate a low mean photon number for μ_0. We use its counting rate instead of Y_0 for the estimation of Y_1, resulting in a lower estimated value of Y_1. This also gives a lower key generation rate.) The ratio of heralding pulses (*i.e.,* gating instances) between the three intensities is about $10 : 4 : 1$. In order to minimize the impact that the

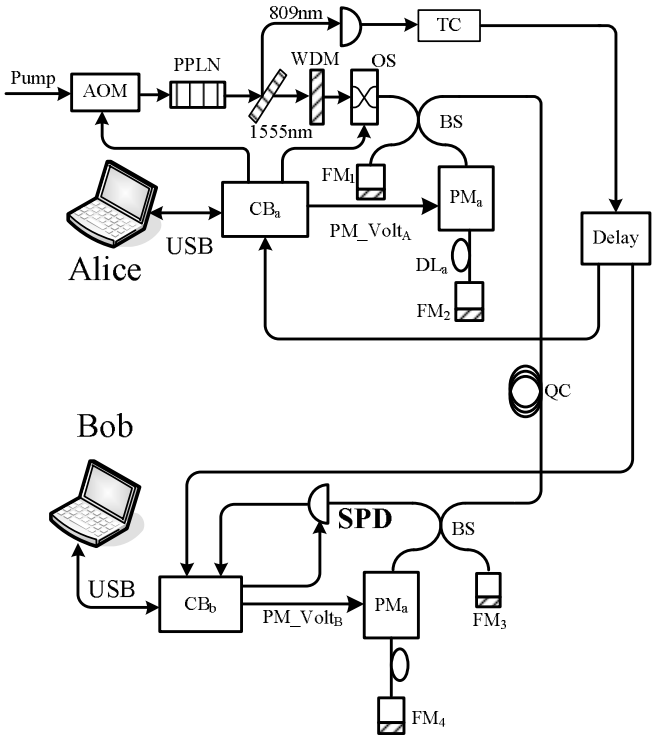

Fig. 3: (Color online) The experimental setup of our quantum key transmission system. PPLN: periodically-poled $LiNbO_3$; AOM: acousto-optical-modulator; WDM: wavelength-division multiplexing; OS: optical switch; TC: time chopper; BS: beam-splitter; FM: Faraday Mirror; PM: phase modulator; DL: delay line; QC: quantum channel; SPD: single photon detector; CB: control board.

power change would have on the triggering rate (since when we change the pump intensity, we change the intensities of both 809 nm and 1555 nm photons), we inserted a fixed dead time after each electrical pulse generated from the Si-APD, calling it time chopper (TC). This way, when the power is increased, the triggering rate does not increase in the same ratio, and according to experimental verification, the dark count probability of our InGaAs APD does not change significantly with the dead time implemented. This dead time was implemented in the software controlling the whole QKD session, and it was also important for our electronic circuit to be able to keep the transmission synchronized. In addition, in order to get a higher visibility in the F-M interferometers ($> 95\%$, without removing any dark counts), we use a wavelength-division multiplexing (WDM) filter to further narrow the bandwidth of the signal photons to 0.4 nm at FWHM. (The spectra measured before the WDM and after the WDM of 1555 nm photons are shown in Fig. 5(a). Fig. 5(b) shows the

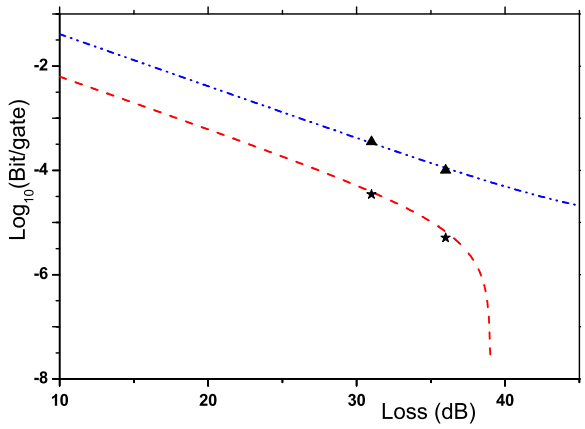

Fig. 4: (Color online) Comparing the theoretical values and experimental results in coincidence counting rate and the final secure key rate. The top line represents the theoretical counting rate for signal photons (μ'); the bottom line represents the theoretical secure key rate (taking statistical fluctuation into account). For each line, we investigated two points at the total loss of 31dB and 36dB individually. The stars and triangles are corresponding experimental results.

interference curve of our F-M interferometer measured with a "strong" light after the WDM filter.)

In our quantum cryptosystem, in order to compensate for the phase-drift in the interferometers caused by the environment, we adopted a scan and transmission mode. The electronic circuit first generates an interference curve, to obtain the correct working voltages for the phase modulators, and then quantum transmission occurs. After a few blocks of data are exchanged, transmission is stopped and scanning recommence to verify if the working point has changed for the next transmission burst, then this pattern follows. For details we refer to [28]. The scan and transmission mode used makes the system quite stable for several hours of continuous measurements. For example, during a typical measurement of 12000 s, (with effective transmission time about 4200 s, the scan and responding time are considerably longer than the transmission time because of the low coincidence count rate), with a total of 1.5 $\times 10^9$ triggering pulses, the detection efficiency is about 7.5%, the "vacuum state" counting rate is about 0.8×10^{-5}/gate, (we attribute 0.7×10^{-5} coming from dark counts, and 0.1×10^{-5} coming from the leakage of the optical switch and the misalignment of the system,) the counting rate, $Q_{\mu'}$ (Q_μ) and average QBER, $E_{\mu'}$ (E_μ) are

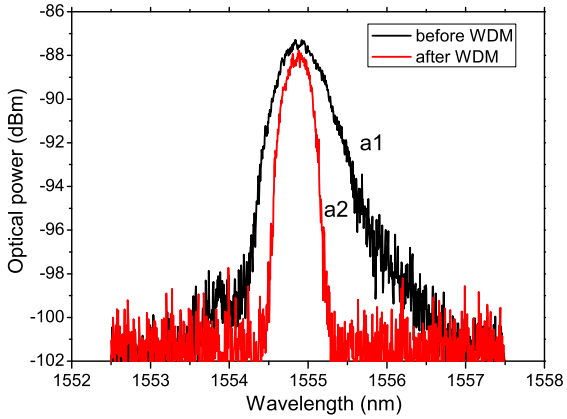

Fig. 5(a): (Color online) Spectra of the signal photons (1555nm) with a strong pump. a1) Measured before the WDM filter; a2) Measured after the WDM filter.

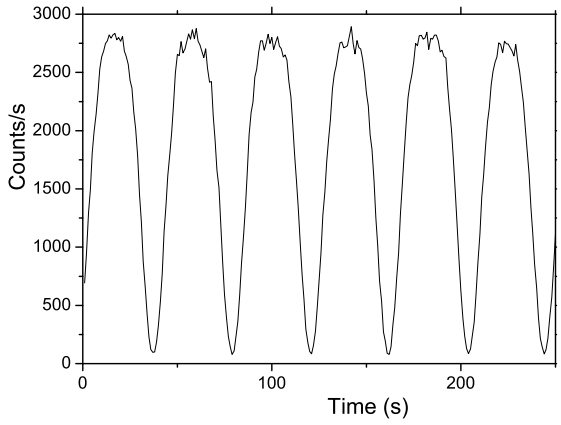

Fig. 5(b): (Color online) The interference curve measured with a "strong" light after the WDM filter passing through our F-M interferometer. (Without removing any dark counts.)

about 1.01×10^{-4} (1.06×10^{-4}) and 6.33% (5.44%) respectively. After a total loss of 36 dB, we get a key generation rate of about 5.065×10^{-6}. Finally, we obtain 5065 secure key bits from a total of 143176 coincidence counts, which agrees well with the theoretical value as shown in Fig. 4 (using a similar simulation model as [20, 22] in our theoretical predictions).

V. CONCLUSIONS AND PROSPECTS

Our final key rate is lower than those in other systems reported [34–38], because there are substantial losses in our present system. Apart from the insertion loss of the WDM filter, the optical switch and a very low detection efficiency of our detector, the main loss comes from the F-M interferometer used, because the signal photons have to go through each phase modulator (PM) twice, and have to suffer losses from two beam-splitters (BS). The aforementioned reasons caused a total loss of about 31 dB. However, using present technology, it's realistic to decrease the loss to a lower value. For example, in order to remove the loss coming from the WDM filter, a narrow bandwidth filter at the wavelength at 809 nm can used at heralding photons instead. This will not only avoid the loss of signal photons, but also increase the correlation rate of photon pairs (it's 70% reported in [27]). Or if a cavity structure is used during the parametric down-conversion processes, it will intrinsically depress the bandwidth of the down-converted light. Moreover, to overcome the loss coming from the F-M interferometer, a low loss Mach-Zehnder (M-Z) interferometer ([38, 39]) can be used instead. Alternatively, if a polarization-coding scheme is used to replace present phase-coding scheme, no interferometer needed, so the scheme will suffer even less loss. In addition, we can also use a better detector at 1555 nm (with a lower dark count probability ($\sim 10^{-6}$) or a higher detection efficiency ($10-15\%$)) or use a two-detector scheme. In all, it's quite realistic to reduce loss by $15-18$ dB with present technology, corresponding to an increased transmission distance of more than 100 km.

In summary, though our present setup still contains many deficiencies, our experimental results are sufficient to in principle demonstrate that our using the HSPS based decoy state scheme could overcome many practical schemes in loss tolerance, which also means it could give a highest key generation rate under fixed loss. Besides, our scheme does not evoke higher costs or other technological requirements than in any other schemes. Therefore, even when practical usability is taken into account, it is still a very promising candidate in the implementation of the quantum cryptography in the near future. (The first three authors-Q. Wang, W. Chen and G. Xavier contribute equally to the work.)

Acknowledgement

Qin Wang is grateful to Prof. X. B. Wang (Tsinghua Univ.) and Dr. C. H. F. Fung (Univ. of Toronto) for fruitful discussions, and Prof. G. Björk for valuable comments.

This work was funded by the EU through the QAP (Qubit Applications-015848) project, and the SECOQC project (FP6-2002-IST-1-506813), the Swedish Science Research Council, the Swedish Foundation for Strategic Research, the ECOC Foundation; and partly funded by the National Science Foundation of China under Grant No. 60537020 and 60621064, Chinese Academy of Sciences and International Partnership Project. G. B. Xavier thanks the Brazilian agencies CAPES and CNPq for financial support.

---

[1] C. H. Bennett and G. Brassard, *in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[3] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[4] D. Mayers, J. ACM **48**, 351 (2001).

[5] H.-K. Lo and H.-F. Chau, Science **283**, 2050 (1999).

[6] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[7] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995); H. P. Yuen, Quantum Semiclassic. Opt. **8**, 939 (1996).

[8] G. Brassard, N. L*ü*tkenhaus, T. Mor, and B. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

[9] N. L*ü*tkenhaus and M. Jahma, New J. Phys. **4**, 44 (2002).

[10] N. L*ü*tkenhaus, Phys. Rev. A, **61**, 052304 (2000).

[11] W. Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[12] X. B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).

[13] H. K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[14] M. Tengner, and D. Ljunggren, e-print quant-ph/0706.2985v1.

[15] H. D. Riedmatten *et al.*, J. Mod. Opt. **51**, 1637 2004.

[16] S. Mori, J. Söderholm, N. Namekata and S. Inoue, Opt. Commun. **264**, 156 (2006).

[17] O. Alibart, D. B. Ostrowsky, P. Baldi, and S. Tanzilli, Opt. Lett. **30**, 1539 (2005).

[18] A. Trifonov and A. Zavriyev, J. Opt. B: Quantum Semiclass. Opt. **7,** S772 (2005).

[19] E. Waks, C. Santori, and Y. Yamamoto, Phys. Rev. **A 66**, 042315 (2002).

[20] Q. Wang, X. B. Wang, and G. C. Guo, Phys. Rev. **A 75**, 012312 (2007).

[21] Q. Wang, and A. Karlsson, Phys. Rev. **A 76,** 014309 (2007).

[22] Q. Wang, X. B. Wang, G. Björk and A. Karlsson, Europhys. Lett. **79**, 40001 (2007).

[23] Q. Wang *et al.,* Phys. Rev. Lett., **100**, 090501 (2008).

[24] We estimated e_1 and Y_1 very conservatively as within 10 standard deviations, which promises a confidence interval for statistical fluctuations of less than 1×10^{-23}.

[25] D. Gottesman, H.-K. Lo, N. L*ü*tkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).

[26] M. Koashi, e-print quant-ph/0609180v1.

[27] A. Zavriyev and A. Trifonov, *in Proceedings of single photon workshop 2007* (Turin, Italy, 2007).

[28] X. F. Mo, B. Zhu, Z. F. Han, Y. Z. Gui, and G. C. Guo, Opt. Lett. **30**, 2632 (2005); Z. F. Han, X. F. Mo, Y. Z. Gui and G. C. Guo, Appl. Phys. Lett. **86**, 221103 (2005).

[29] M. J. LaGasse, Secure use of a single single-photon detector in a QKD system, United States patent application 20050190922 (2005).

[30] B. Qi, C. H. F. Fung, H. K. Lo, and X. F. Ma, Quantum Inf. Com. **7**, 073 (2007)

[31] Y. Zhao, C. H. F. Fung, B. Qi, C. Chen, H. K. Lo, e-print quant-ph/0704.3253.

[32] V. Makarov, J. Skaar, e-print quant-ph/0702262.

[33] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. **A 73**, 022320 (2006).

[34] Y. Zhao, B. Qi, X. F. Ma, H. K. Lo, and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006).

[35] D. Rosenberg *et al*, Phys. Rev. Lett., **98**, 010503 (2007).

[36] T. Schmitt-Manderbach *et al.*, Phys. Rev. Lett., **98**, 010504 (2007).

[37] C. Z. Peng *et al.*, Phys. Rev. Lett., **98**, 010505 (2007).

[38] Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **90**, 011118 (2007).

[39] P. M. Intallura, M. B. Ward, O. Z. Karimov, Z. L. Yuan, P. See, and A. J. Shields, e-print quant-ph/0710.0565.